Topics:

Information Security Control Policy [1]

PURPOSE

The purpose of this policy is to improve how security controls are managed within the State?s shared-service environment. Security operations remains a top priority and is necessary to continue to advance security practices and processes. The definition of ?ownership? within a shared-services environment has different dimensions. As it pertains to security, controls are often established by agency business owners but are typically executed by multiple parties. Often times the delineation of duties between multiple parties are not clearly understood resulting in inconsistencies in the execution of responsibilities. The Security Control Policy addresses this business challenge by establishing clearer lines of delineation between security controls, ownership and the overall responsibility of execution.

SCOPE and AUTHORITY

This policy covers the following:

- Full service agencies who receive Infrastructure Services and Managed Network Services from the State Data Center

- Agencies who receive only Managed Network Services from the State Data Center

- Agencies who receive services from third-party service providers and those that own and operate their own Infrastructure/network services environment.

Information Technology Policies, Standards and Guidelines (PM-04-001) [or add: Enterprise Information Security Charter (PS-08-005)]

POLICY

Agencies, Service Providers and Service Integrators will comply with all applicable NIST Security Controls (or any other Industry standards) that are required for state and federal compliance. These controls listed in standard SM 17-001 will be outlined in more detail within the NIST Control Families, Technical, Operational and Managerial Controls. Security controls will be determined and aligned using the State?s application/system classifications of Low, Moderate and High. After which each entity will work within this control framework to identify the appropriate security controls to support the application and system portfolio being managed. Once control ownership is identified, the controlling owner will be responsible for the implementation and management of the identified control(s). All controls identified as ?shared? will be co-owned between two or more entities that together assume the responsibility for the execution of the control(s). The expectation is that agencies, service providers and service integrators will work together within the